# STAFFING INDIA'S CYBER WORKFORCE:

# DEVELOPING A MULTI-DIMENSIONAL CYBER TALENT-SELECTION MODEL

SHORT SYNOPSIS

Submitted in partial fulfilment of the requirement of the degree of

DOCTOR OF PHILOSOPHY

to

Manav Rachna International Institute of Research and Studies

(Deemed to be University)

by

Ramesh Balan
Registration No: 19/PhD/065

Under the supervision of

Dr. Nandini Srivastava, Professor & Director - Council for Doctoral Program (CDP)

FACULTY OF MANAGEMENT STUDIES

MANAV RACHNA INTERNATIONAL INSTITUTE OF RESEARCH & STUDIES

SECTOR-43, SURAJKUND –DELHI ROAD, FARIDABAD – 121001

**FACULTY OF MANAGEMENT STUDIES**

**Certificate**

I hereby declare that the short synopsis entitled "Staffing India's Cyber Workforce: Developing a Multi-Dimensional Cyber Talent-Selection Model" is being submitted in partial fulfilment of the requirement for the degree of Doctor of Philosophy in Management under Faculty of Management Studies of Manav Rachna International Institute of Research & Studies, Faridabad during the academic year 2020-21. It is a bona fide record of original work carried out under the supervision of Dr. Nandini Srivastava, Professor & Director - Council for Doctoral Program (CDP), MRIIRS, Faridabad, and has not been submitted in full or part to any other university or institute for degree or diploma. Further, it is certified that this short synopsis is plagiarism free and proof has been submitted.

(Ramesh Balan)
Registration No: 19/PhD/065

Dr. Nandini Srivastava,
Professor & Director - Council for Doctoral Program (CDP)
MRIIRS, Faridabad

(Chairperson, DRC)

(Chairperson, CDP)

**Abstract**

Operating in and securing the cyber domain in the information age has become critical for the nation. In fact, in many nations the cyber domain has been categorised as a strategic sector. Even so, the employment of talent management theories/ practices towards creation of a cyber workforce for India, has thus far drawn scant attention *vis a vis* the policy and technology dimensions of the discourse.

Cyber talent is scarce and falls short of demand, resulting in fierce competition for it. Deliberations on the matter are constrained by its nascence, security considerations, extant organisational culture, and the methodology of selection, sustenance and retention of talent; coupled with nebulous job/ role characterisation.

Over time a few individual approaches to talent-selection have attained prominence. They are based on ability/ knowledge, aptitude, interests, and personality (occupational behaviour, attitudes, etc.). In this backdrop, there is scope to develop a multi-dimensional cyber talent-selection model for the staffing India's cyber workforce which is capable of effectively addressing talent selection, based on a matching characterisation of cyber job-roles. Developing such a model will be focus of this research.

Key Words: Cyber, workforce, dimension, human capital, interpersonal skills, self-motivation, employee profiling.

## CONTENTS


| S. No. | Description | Page No. |
|---|---|---|
| 1 | Introduction | 6-7 |
| 2 | Literature Review | 8-22 |
| 3 | Description of Broad Area | 23 |
| 4 | Objectives of the Study | 24 |
| 5 | Methodology | 24-25 |
| 6 | Expected Outcome of the Research | 26 |
| | References | |
| | Plagiarism Report | |

1. **Introduction**.

1.1. **Cybersecurity: A Strategic Sector**.

Information is a crucial lever of national power, being intricately inter-twined with all the remaining levers viz., politico-diplomatic, military and economic; and within that, the field of cybersecurity is crucial to today's knowledge economy – because it relates to the basic characteristics of information, viz., confidentiality, integrity and availability. Further, of late 'cyber' is also being viewed as a domain of warfare. Thus, cyber security is heading towards designation as a strategic sector for the nation. In this backdrop, India's draft National Cyber Security Strategy rightly prioritises among other things - the cyber security workforce. This appears to endorse the view that cyber security is more a human problem than a technology one (Singer & Friedman, 2015).

1.2. **Cyber Security Workforce**.

Reference to scholarly works and open-source literature indicates a global war for talent, triggered by scarcity and shortfall (Chambers et al., 1998). Therefore, for a manager (of cyber talent), hiring is the single most important thing he needs to do at work (Schmidt & Rosenberg, 2014). Hence, sustained capacity-building in terms of a professional cyber workforce, merits our urgent, and foremost consideration (Fortson, 2017). In this backdrop, cyber talent management in general and cyber talent selection in particular gain prominence. Without getting into further details at this stage, cyber talent needs to be selected to fit job/ roles which answer to the broad descriptions of analysis, (e.g., forensics, malware analysis, intrusion analysis, cyber threat intelligence analysis), operations (e.g., incident response, operations), testing (e.g., penetration testing, vulnerability assessment), architecture (e.g., cyber security advise), and maintenance (e.g., system administration) – in both the offensive and defensive arenas of cyber security.

1.3. **Researcher's Appreciation of Prevailing Approach to Cyber Talent Selection**.

As per this researcher's appreciation, globally there is no established career growth path in the cyber domain; staffing is tackled in a functional rather than structured manner; and cross-disciplinary requirements are not fully catered to. Candidates are currently assigned to cyber billets, based on prior training or past experience, or acquired qualifications/ certifications or references. Scant attention is paid to his/ her aptitude and competence. Likewise, the candidate's social/ emotional intelligence, personality, interest congruence or team spirit are not systemically factored in. This is principally because existing models

of talent selection are either not designed to meet the unique needs of the cyber field, or they are not scalable, or they are not robust. Meanwhile, as the field continues to grow in prominence, demand continues to outstrip supply, progressively accentuating the felt need. The issue thus warrants a fresh look, in order to mitigate the gap, particularly in the Indian context.

### 1.4. **Cyber Talent Selection: A Systematic Approach**.

Starting from the basics, it may be seen that talent selection in any domain involves constructs such as mental ability; personality; interests, values & fit; knowledge; work skills; social skills; and physical characteristic; and corresponding methods such as biodata/ CV/ resume/ applications, interviews, references etc for assessment (Cook, 2016). The inference is that application of a multi-dimensional talent selection model (e.g., human capital, inter-personal skills, self-motivation/ interest-congruence, and employee profile) to the cyber domain will yield better selection choices; and potentially, improved job performance. Literature review shows the existence of a few multi-dimensional models. Examination of their suitability and their extension appears to hold promise for the Indian context. Such a model can also possibly be extended to cover the selection of prospective candidates ranging from freshers to mid-career lateral inductees, to service a diverse range of cyber organisations.

## 2. **Literature Review**.

This research is based on **three planks of a triad,** as shown below, and described in subsequent paragraphs, viz.,

1) understanding of job performance;
2) review of job/role characterisation; and
3) study of cyber talent selection models.

### 2.1. **Job Performance**.

2.1.1. ***Dependency*** - Superior job performance is a payoff one may expect from appropriate talent selection based on accurate job/ role characterisation. This is depicted schematically, in *Figure 1* below.

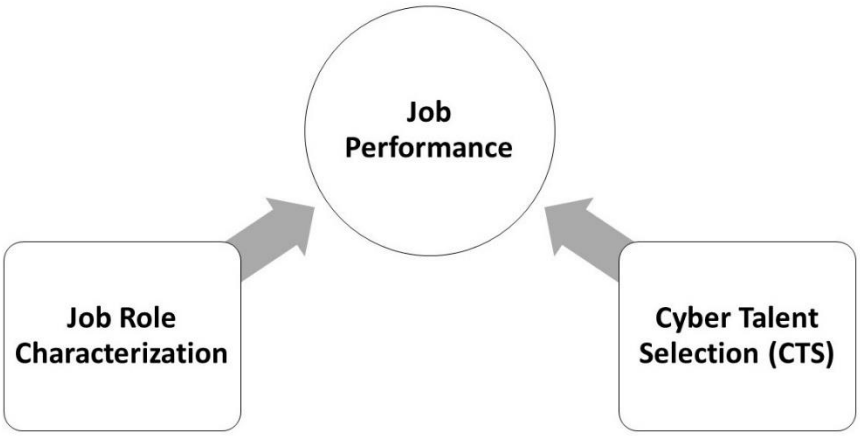


*Figure 1: Job Performance as a function of Job/ Role Characterisation and Talent Selection, as conceived by the Researcher*

2.1.2. **Antecedent Factors** - To begin with it must be noted that job performance is not a static entity, and is subject to change. In itself, it is the outcome of antecedent factors such as task performance, contextual performance and adaptive performance (Mueller-Hanson & Garza, 2016). The first two of these antecedent factors is reinforced (Borman & Motowildo, 1993). However, the third antecedent factor is replaced in some works by counterproductive work behaviour – "any intentional behaviour on the part of an organization member viewed by the organization as contrary to its legitimate interests" (Sackett & DeVore, 2001). As far as measurement of job performance is concerned, assessments made by superiors in the chain appears to be popular (Sjöberg, 2014). The assessment model can be quantified in terms of nine dimensions of job performance (Viswesvaran et al., 2005). This can be complemented by dwelling on eight distinctive dimensions of adaptive performance i.e. the third antecedent factor

(Pulakos et al., 2000). The first six of these eight distinctive dimensions are relevant to cybersecurity job roles (Mueller-Hanson & Garza, 2016).

2.1.3. **Consolidated Dimensions of Job Performance** - Consolidated dimensions of job performance are as shown below at *Table 1.*

| Dimensions of Job Performance Rating (Viswesvaran et al., 2005) | | Dimensions of Adaptive Performance (Pulakos et al., 2000) | |
|---|---|---|---|
| 1. | Interpersonal Competence | *1.* | *Handling Emergencies* |
| 2. | Administrative Competence | *2.* | *Handling Work Stress* |
| 3. | Quality | *3.* | *Solving problems creatively* |
| 4. | Productivity | *4.* | *Dealing with uncertain situations* |
| 5. | Effort | *5.* | *Learning work tasks, technologies, and procedures* |
| 6. | Job-Knowledge | *6.* | *Interpersonal adaptability* |
| 7. | Leadership | 7. | Cultural adaptability |
| 8. | Compliance/ Acceptance of Authority | 8. | Physically oriented adaptability |
| 9. | Communication Competence | - | - |

*Table 1: Consolidated Dimensions of Job Performance (Viswesvaran et al., 2005) and (Pulakos et al., 2000)*

2.2. **Job Roles/ Characterisation**.

Since cyber talent selection is closely related to the job/ role for which the prospective candidate is being screened, it is important to understand how job/ role characterisation in this domain is carried out; nuances of which are described in succeeding paragraphs.

### 2.2.1. **Dimensions of Job/ Roles Characterisation**.

Job/ role characterisation can be attempted along the dimensions shown in *Figure 2* below:

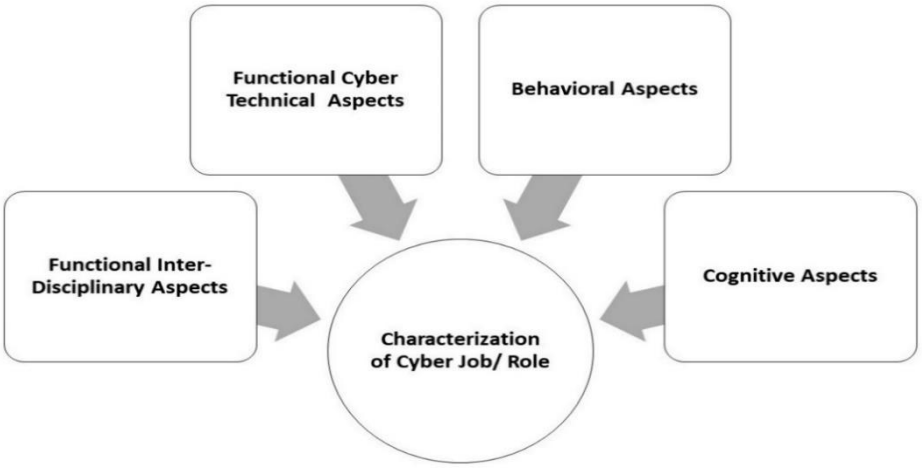


*Figure 2:Dimensions of Job Role Characterisation, as conceived by the Researcher*

### 2.2.2. **Frameworks: Job/ Roles Characterisation**.

Quite a few frameworks for job/ roles characterisation in cyber domain exist. Prominent amongst these are mentioned below: -

1) U.S.' NCWF, 2017;
2) E.U.'s SPARTA, Cybersecurity Skills Framework 2020; and
3) Australia's Cyber Skills Framework, 2020.

These are briefly described in succeeding paragraphs, as follows: -

a) **U.S.' NCWF, 2017** - Job/ roles in the cyber domain has been examined in the NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework (NCWF – where the letter 'N' represents NICE) (also called NICE Framework), which was put out by NIST (National Institute of Standards and Technology) and DHS (Department of Homeland Security) in the United States (Caulkins, 2018; Jacob et al., 2018; Newhouse et al., 2017). The NICE Framework enables consistent understanding of cybersecurity work roles (exhibited in terms of relevant experience, and pedagogy), by use of a common language, and thus links training, and education with job characterisation, and industry needs. Work roles can be enumerated in terms of attributes (captured in terms of KSAs - knowledge, skills, and abilities) and decomposed into tasks (a defined pieces of work - performed in that role). Hence, task is the basic building block. Related tasks, when

grouped together compose work roles in a specific speciality area, which in turn, when combined, yield categories. NCWF (Newhouse et al., 2017) caters for 1007 tasks attributable to roles, and generates a matrix of 630 knowledge items across 374 skills, and 176 abilities. Insofar, it is overwhelming in its depth of detail. Though flexible and extensible by design, it naturally adheres to U.S. standards, legal framework and regulations. Hence its adoption by other countries can be viable only post-customisation. One of its drawbacks is that it does not cater for different levels of proficiency of candidate-skills. Another observation relates to lack of clarity regarding its ability to cater for emerging skills/knowledge levels, *vis a vis* currently existing one. It also does not characterise non-technical job roles. However, notwithstanding these drawbacks, it is a tremendous reference and a pioneering one at that.

**b) E.U.'s SPARTA, Cybersecurity Skills Framework 2020** - The E.U. has published a comparable framework called SPARTA (Strategic Programs for Advanced Research and Technology in Europe) (Piesarskas, 2020) Cybersecurity Skills Framework. It is a derivative of the U.S.' NCWF described above, but has been customised to E.U.'s legislative and practical requirements.

c) **Australia's Cyber Skills Framework, 2020** - Likewise, the Australian Signals Directorate (A.S.D.) has published Cyber Skills Framework (ASD, 2020), which is comparable to a substantially simplified version of the U.S. NCWF. In addition, it caters for competency criteria - to match national public service levels - and provides for proficiency levels, career pathways and learning & development pathways.

d) As the field is yet evolving, there are other analogous and emerging models. However, a study of just these three is adequately illuminating. Highlights of U.S. NICE Framework (2017), E.U. SPARTA CS Framework (v0.9, 2020) and A.S.D. Cyber Skills Framework (v2.0, 2020) are shown in *Table 2* below: -

| **Parameters** | **Cyber Security Workforce/ Skills Frameworks under Consideration** | | |
|---|---|---|---|
| Chief Features Describing the Framework | U.S. NCWF or NICE Framework (2017) | E.U. SPARTA Cybersecurity Skills Framework (v0.9,2020) | Australian Signal Directorate Cyber Skills Framework (v2.0, 2020) |
| Categories (high-level grouping of common cybersecurity functions) **or** Cyber Role Definitions | 07 | 07 | 09 |
| Specialty Areas (distinct areas of cybersecurity work) **or** Capability and Skill definitions | 33 | 33 | 09 |
| Work Roles (detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSAs) required to perform tasks in a Work Role) | 52 | 54 | - |
| Proficiency Levels | - | - | 06 |
| Career Pathways | - | - | 04 |
| Learning and development pathway | - | - | 01 |

*Table 2: Highlights of U.S.' NICE Framework (2017), E.U.'s SPARTA Cybersecurity Skills Framework (v0.9, 2020) and Australia's. Cyber Skills Framework (v2.0, 2020)*

2.2.3. **Deductions** - Although the NCWF, 2017 forms a useful reference, it is too voluminous in its detail. Hence, for the purpose of this study a subset of job categories and roles - principally extracted from the A.S.D. Cyber Skills Framework, 2020, but duly supplemented (by a few out of NCWF, 2017) - could be considered, working on the premise that this approach is extensible to other job categories. Such a subset of proposed job categories/ roles is dwelt upon a little further in this paper.

2.3. **Cyber Talent Selection Models**.

Based on the literature review undertaken, six multi-dimensional models for cyber talent selection as follows have been identified; which are listed in *Table 3* below: -

| S. No | Name of Model | References |
|---|---|---|
| 1. | Cyber Aptitude and Talent Assessment (CATA) Framework | (Campbell & Bradley, 2018; Campbell et al., 2016a, 2016b; Morris & Waage, 2015; Saner et al., 2016) |
| 2. | Cyber Assessment & Selection Programme (CASP) | (Morris & Waage, 2015) |
| 3. | Distal-Proximal Attributes Model | (Jose et al., 2016) |
| 4. | N.E.C.'s Cybersecurity HR Talent Management Model | (Minegishi, 2018) |
| 5. | Delphi Top Ten Factors Model | (Galliano, 2017) |
| 6. | Multi-Stage - Multi-Level Model | (Mueller-Hanson & Garza, 2016) |

*Table 3: List of Identified Multi-dimensional Cyber Talent Selection Models, based on Literature Review by the Researcher*

2.3.1. **Brief Description: Cyber Aptitude and Talent Assessment (CATA) Framework**.

One of the models listed in Table 3 above, viz., the CATA framework, is described briefly in succeeding paras. The CATA framework is aimed at identifying dimensions of cyber aptitude in a prospective candidate. Major nuances of the CATA Framework are as follows: -

**Background** - The model is premised on knowledge-based evaluation of candidates who have cognitive suitability, but may not yet have had the opportunity/ exposure to learn. The process can be broken down as shown below: -

I. Using the job categorisation given in the NCWF (Newhouse et al., 2017), the CATA framework first matches the personal attributes - beyond general mental ability (GMA) (Cronbach, 1990; Lubinski, 2000; Meehl, 1990; Schmidt & Hunter, 1998)) - of a prospective candidate, to the job role/ profile. This is done in terms of

antecedent factors such as 1) *Critical Thinking* (IQ) - in terms of (a) reasoning & (b) working memory; and 2) *Job Specific Components* – in terms of (a) *Deliberate/ Real Time Action &* (b) *Proactive/ Reactive Thinking.*

II. The framework next attempts to predict the presence of Cyber Aptitude (Snow, 1978, 1992) in a prospective candidate.

**Methodology -** Psychometric tests as shown in *Table 4* below are proposed for data collection. Details of operationalisation of the concept on a two axes graph, are shown in *Figure 3* below. Data collection details have not been shared, on grounds of being proprietary. Sampling method has also not been shared. Method of data analysis, and findings have not been shared. Interim results related to reliability and validity of the model, have been discussed only in part, that too qualitatively.

| **Section** | **Construct** | **Test** |
|---|---|---|
| Critical Thinking | Visuospatial Working Memory | Shapebuilder |
| | Rule Induction | Letter Sets |
| | Complex Problem-Solving | Dynamic Systems Control |
| | Spatial Visualization | Paper Folding |
| | Attentional Capacity | Shape Comparison |
| Deliberate Action | Need for Closure | Need for Cognitive Closure |
| | Tolerance for Risk | Balloon Analogue Risk Task |
| Real-Time Action | Psychomotor Speed | Recent Probes (1 item) |
| | Pattern Recognition and Scanning | Decoding Speed |
| | Resistance to Interference | Recent Probes (4 & 9 Items) |

*Table 4: CATA Section, Constructs & (Psychometric) Tests (Morris & Waage, 2015)*

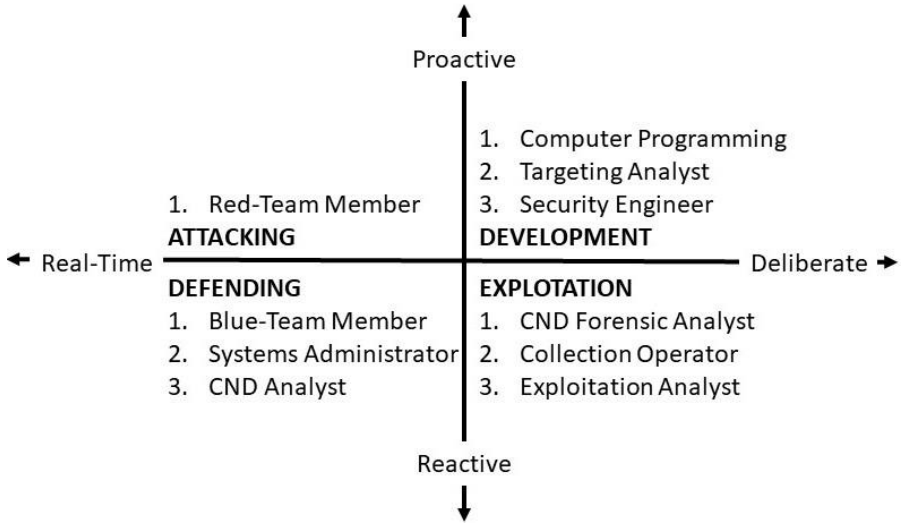


*Figure 3: CATA Framework - Job-specific Model, with Particular Jobs Identified based on (Campbell & Bradley, 2018)*

**Critique –** The model has not been empirically validated, as per literature published upto 2018. Also, at least some of the psychometric tests utilised appear to be proprietary.

2.3.2. **Summarised Description**. A summarised description of all the six models listed at Table 3 above is tabulated at *Table 5* below.

| **Model Name** | **Antecedent Factors** | **Outcome Factors** | **Empirical Validation** |
|---|---|---|---|
| CATA Frame-work | No of Constructs: 02<br>Antecedent Factors:<br>1) Critical Thinking (IQ) in terms of reasoning and working memory;<br>2) Job Specific Components, viz, (a) Deliberate/ Real Time Action; (b) Proactive/ Reactive Thinking. | Identification of Cyber Aptitude | ✓ Not empirically validated, current upto 2018.<br>✓ Some psychometric tests appear to be proprietary |
| CASP | No of Constructs: 03<br>Antecedent Factors:<br>1) Cognitive Ability.<br>2) Aptitude – assessed through exhibition of creativity.<br>3) Competence. | Selection of potential cyber personnel | Not empirically validated, current upto 2015 |

| Model Name | Antecedent Factors | Outcome Factors | Empirical Validation |
|---|---|---|---|
| Distal-Proximal Attributes Model | No of Constructs: 06<br>Antecedent Factors:<br>1) Distal Attributes. (a) Cognitive Ability; (b) Motivation (Interest Congruence); (c) Personality.<br>2) Proximal Attributes. (a) Competence (Technical Skills); (b) Personality/ Emotional Intelligence (Social Skills); (c) Aptitude (as seen through the lens of Problem Solving). | Selection of potential cyber personnel | Not empirically validated, current upto 2016 |
| N.E.C.'s CS HR TM Model | No of Constructs: 02<br>Antecedent Factors:<br>1)Qualification.<br>2) Competence. | Talent management of cybersecurity human resources | Empirically validated; however not described, current uto 2017 |
| Delphi Top Ten Factors Model | No of Constructs: 06<br>Antecedent Factors:<br>1) Character Traits (Integrity, loyalty, honesty, and others).<br>2) Aptitude (Critical Thinking and Data Analysis Skills, Curiosity and Desire to Learn).<br>3) Background checks and reference validation.<br>4) Personality (Soft skills, social skills, and people skills).<br>5) Mental Ability (Industry-recognized certifications, Educational Qualifications, Translating governance, policy, and regulations to the business).<br>6) Competence (Hands on Skills, Knowledge exams). | Selection of cybersecurity professionals (assessing and matching candidates) to cybersecurity job openings. | Not empirically validated, current upto 2017 |

| Model Name | Antecedent Factors | Outcome Factors | Empirical Validation |
|---|---|---|---|
| MSML Model | No of Constructs: 06<br>Antecedent Factors:<br>1) Cognitive Skills, in terms of (a) Numerical Reasoning; (b) Inductive Reasoning; (c) Spatial Relations; (d) Perceptual Speed.<br>2) Personality, in terms of (a) Dependability; (b) Agreeableness; (c) Openness to Experience; (d) Interpersonal Skills - specific (relevant to the role) and generic (oral communication, interpersonal sensitivity etc).<br>3) Competence, in terms of Technical Knowledge and Skills, which may either be specific (relevant to role) or generic (e.g., analysis, evaluation oriented).<br>4) References, in terms of experience, with the following measurable parameters, viz., (a) Performing relevant tasks; (b) Performing in relevant contexts; (c) Adapting to change.<br>5) Teamwork – measurable in terms of Transportable attributes, and Contextual attributes. Transportable attributes in turn are measurable in terms of (a) Collectivism (Desire for group solidarity and preference toward teamwork); (b) Personality (Emotional Stability, Agreeableness, Conscientiousness); (c) Teamwork Knowledge & Skills – with seven sub-components, viz., (1) morale building, (2) conflict resolution, (3) information exchange, (4) task motivation, (5) cooperation, (6) consultation with others, and (7) assertiveness). However, Contextual attributes are measurable in terms of (a) Team cohesion; (b) Transactive memory; (c) Shared mental models. | Selection of potential cyber personnel - measured by job performance, measured in turn by task, contextual and adaptive performance respectively. | Not empirically validated, current upto 2016 |

*Table 5: Summarised description of all the six models, based on Literature Review by the Researcher*

2.3.3. **Conceptual Findings**.

I. All the identified models are designed around a range of antecedent factors/ dimensions. The following antecedent factors appear to be common across the six considered models, viz., *1) human capital* -which is deemed to be an amalgam of a) cognitive ability; b) competence; and c) aptitude (measured by critical thinking, problem solving, creativity, curiosity, reactive/ proactive actions, and deliberate/ real-time actions); *2) interpersonal skills* - which is a combination of a) personality and social skills; and b) character traits; *3) motivation/ interest congruence*; and *4) employee profile* - which is captured in terms of a) qualifications/ credentials; and b) references (background experience and training). *Character traits* of a prospective candidate appear to be a crucial input for any organisation. *Teamwork* seems to be important for at least some, if not all cyber job roles.

**II.** Although technical proficiency is a necessary, but not sufficient condition for tenanting cyber job roles, all the considered models have restricted themselves to only the technical dimensions of cyber job roles.

III. CATA section, constructs, & (psychometric) tests - rely on a number of psychometric tests, some of which may well be proprietary. Hence, if the concept is to be used, the need to improvise using alternate open domain tests may arise.

IV. Almost all models have been designed for selection of cyber personnel. The CATA Framework places aptitude as the outcome factor, which serves as an antecedent factor for several other models.

V. A common theme with respect to the overall outcome factor appears to be measurability in terms of job performance. In this connection, construction validation methods are relevant.

VI. For any given set of antecedent factors, discussed above, construct validation can be attempted using a variety of methods (Cook, 2016).

2.4. **Description of Conceptual Framework**.

From the extant literature survey, the following section presents the description of the identified dimensions pertinent in the context of cyber talent workforce. The variables have also been identified and put forward which would help the researcher in building the survey instrument. Details are as follows: -

2.4.1. **Human Capital.** While there is no single agreed upon definition of human capital, it can be taken to connote both innate and acquired skills, competence, and ability (Kucharcikova, 2011; Patrick M. Wright, 2011). For the purposes of this research, it will be deemed to comprise of a combination of the following: -

**a. Cognitive Ability** - Cognitive ability may be defined as a "mental capability that … involves the ability to reason, plan, solve problems, think abstractly, comprehend complex ideas, learn quickly and learn from experience (Gottfredson, 1997, p. 13)". (Batey & Hughes, 2017)**.**

b. **Aptitude** - Aptitudes are psychological constructs about individual differences in learning or performance in specified situation" (Snow, 1992). It can be construed as "…innate potential to do certain kinds of work - whether or not yet developed - at a certain level; … and is thus in contrast to skills and achievement, which represent knowledge or ability that is gained through learning". "Aptitude testing may be used to gauge general readiness" (Campbell et al., 2016b), (Galliano, 2017). In the current context, it can contribute to prediction of success in cybersecurity (Shuftan & Michaud, 2016).

*c.* **Competence** - when applied to the cyber domain - connotes the hands-on capability of a candidate to apply his knowledge to produce organisational outcomes. It draws authority from "Testing for Competence Rather Than for Intelligence" (McClelland, 1973).

2.4.2. **Interpersonal Skills**. For the purposes of this research, interpersonal skills will be deemed to comprise of a combination of the following: -

*a.* **Personality** - Individual differences in characteristic sets of … relatively stable, behaviour (e.g., interpersonal behaviour), cognition, and emotional patterns (e.g., motivations or teamwork) …", as also how the various parts of a person come together as a whole. Along with cognitive ability (intelligence or general mental ability), personality traits (such as leadership, character, teamwork, and so on) play an important role in predicting job performance.

b. **Character Traits** - Character traits are distinguishing and valued attributes of a candidate's personality and behaviour – such as honesty, integrity, loyalty and such others.

2.4.3. **Self-Motivation/ Interest Congruence** - The concept of interest can be viewed from three perspectives: (1) its motivational role (direction, vigour, persistence), (2) its behavioural outcomes (selection and performance), and (3) its affective and cognitive dimensions (Su, 2020). "Interests influence the types of environments we seek and the types of people and activities we prefer… [but] understanding the person's interests will not likely enhance our understanding of how we do work" (Barrick, 2005). It is believed that "interests and interest congruence predict a broad range of outcomes, including educational and occupational choice, persistence (stability), satisfaction, and achievement" (Holland, 1992). The aspect of congruence is appended to interest to typify agreement with a model of interest types (RIASEC) put out by John Holland.

2.4.4. **Employee Profiling**. For the purposes of this research, employee profiling will be deemed to comprise of a combination of the following: -

- ✓ **Credentials** - Credentials will be viewed as qualifications in terms of educational background (domain of knowledge and/ or proficiency), or certification in terms of training, to indicate a candidate's suitability for a job/ role.
- ✓ **References** - References will denote the inferences which can be derived from a candidate's experience, training, spoken reputation, performance appraisals, professional and social feedback (e.g., work experience, work habits, character and skills) etc.

2.5. **Conceptual Framework**.

In light of the theoretical framework(s) analysed above, the following conceptual framework is proposed: -

2.5.1. **Cyber Talent Selection**. A multi-dimensional model for cyber talent selection, as depicted schematically in *Figure 5* below, is proposed. Suitable

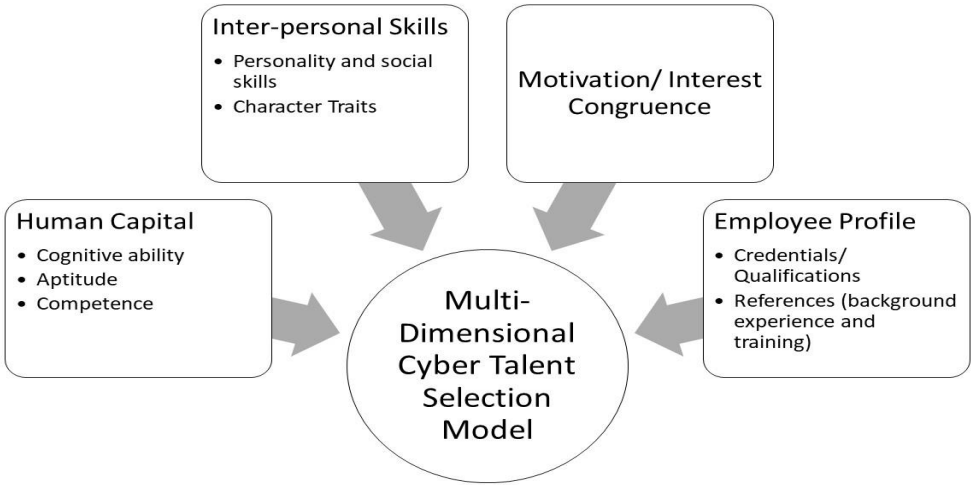


*Figure 4: Multi-dimensional Cyber Talent Selection Model, as conceived by the Researcher*

weights can be assigned to each of the dimensions of cyber talent selection (antecedent factors), based on relative importance and context (driven by organisational needs, which may change with passage of time) thus, making the model generalisable across diverse cyber organisations.

2.5.2. **Job/ Role Characterisation**.

The subset of job categories/ roles proposed to be utilised for the purpose of this research is as follows.

**Base Categories and Roles** - based on A.S.D. Cyber Skills Framework, 2020.

1. Cybersecurity Analysis Roles - Cyber Threat Analyst, Intrusion Analyst, and Malware Analyst.
2. Cybersecurity Operations Roles - Incident Responder, and Operations Coordinator.
3. Cybersecurity Testing Roles - Penetration Tester, and Vulnerability Assessor.
4. Cybersecurity Architecture Roles - Cybersecurity Advice & Assessment, and Vulnerability Researcher.

**Supplementary Categories and Roles** - based on NCWF, 2017.

1. Operations and Maintenance Role - Systems Administrator.
2. Analysis Roles - Exploitation Analyst, Target Developer, and Targeting Network Analyst.

**Characterisation** - Characterisation of jobs related to the roles identified above are essentially a paraphrasing/ reproduction of the job descriptions/ expectations stated in (ASD, 2020; Newhouse et al., 2017).

2.5.3. **Job Performance**.

Consolidated dimensions of job performance as previously shown at *Table 1,* will be adopted for the purpose of this research.

2.6. **Research Gap**. The study is an attempt to conduct research in the domain of cyber talent workforce in Indian context. With increasing challenges in the cyber world, for example threat to data security, and data protection etc., there is utmost need to recruited skilled workforce. The purview of the study is to examine the essential traits and attributes required in the workforce to productively serve in cyber assignments.

2.7. **Desirable Characteristics of the Model**. The model should be flexible enough to cater for diverse selection priorities across organisations and across time (based on internal strengths/ weaknesses *and* external opportunities/ threats). If an organisation for instance, has a *surge requirement* for trained cyber talent, for immediate prosecution of cyber operations, it may place a greater premium on (current) ability and qualifications *vis a vis* aptitude (trainability and potential ability). On the other hand, if the *cyber talent catchment area* does not throw up sufficient numbers of competent, prospective cyber talent for any reason whatsoever, then the very same organisation may be constrained to prioritise aptitude and trainability, over current ability and competence - provided it can afford the time and resources to develop the candidates in the long run. A *flexible model* can also help an organisation to differentially focus on long term building of the cyber talent pipe-line, even as it continues to meet short term operational requirement. Insofar, it may choose to select permanent employees for the core nucleus - based on aptitude, and trainability, while it picks up temporary employees for the support cadre - based on ability, and hands on competence.

3. **Description of Broad Area**.

Cyber security which is emerging as a strategic sector, is heavily dependent on the quality of human resource involved in the domain. Hence, there is need to focus on cyber-talent selection for characterised jobs/ roles, to realise superior job performance. Based on the conceptual framework developed in preceding paragraphs it appears that there is scope to develop a Multi-dimensional Cyber Talent-selection model for the staffing of India's cyber workforce. The model should be flexible enough to cater for diverse selection priorities across organisations and across time (based on internal strengths/ weaknesses *and* external opportunities/ threats).

4. **Objectives of the Study**.

4.1. **Research Questions**. Based on the literature review undertaken, the following research questions arise: -

4.1.1. What are the dimensions of cyber talent selection?

4.1.2. Which among the identified dimensions to select cyber talent are more prevalent?

4.1.3. Do the dimensions of cyber talent selection predict employee job performance?

4.2. **Enumeration of Objectives**. Objectives are enumerated as follows: -

4.2.1. To explore the dimensions of cyber talent selection.

4.2.2. To measure the extent of utilization of the identified dimensions for selecting cyber talent.

4.2.3. To examine the significance of the dimensions of cyber talent selection for employee job performance.

4.2.4. To propose a multi-dimensional selection model for staffing Indian cyber workforce.

5. **Methodology**.

5.1. **Research Design**. The study will follow descriptive research design. The factors and variables have been identified with the help of literature review. Primary data will be collected with the help of survey method using a validated instrument (questionnaire).

5.2. **Population**. The survey population for the research study is the aggregate of practicing cybersecurity professionals and business owners/ drivers of cyber security (e.g., Chief Information Security Officers (CISO), or Information Security Managers (or equivalent)) working in public and private sector organizations principally engaged in the field of cyber security.

5.3. **Sampling**.

*5.3.1.* **Sampling Unit** - To make the study applicable at the national level, data will be collected from employees working in both the public and private sector organizations. Stratified RANDOM sampling will be used to draw the sample elements from the population.

*5.3.2.* **Sample Size** - The estimated sample size is nearly 250. However, the exact sample size will depend on the survey items of the instrument. There would be at least 5-10 observations per item as per (Bentler & Chou, 1987; Bollen, 1989; Nunnally & Bernstein, 1994).

*5.3.3.* **Potential Respondents** – Based on survey of literature (Chhibbar, 2020; DSCI & PwC, 2019; Saraswat, 2019), and personal interaction with representative of ISAC, India (https://www.isacindia.org/) during May-June 2021, a representative list of potential respondents has been drawn up; and is shown below: -

| PMO | MHA | MOD | MEA |
|---|---|---|---|
| NSCS | I4C | DRDO | CSG |
| R&AW | LEA – IB | HQ IDS | |
| NTRO | C&IS Div | Army | |
| NCIIPC | CIDR/ UIDAI | Navy | |
| | TETRA | Air Force | |
| | NATGRID | | |
| | NCCC | | |
| | Dte of Forensic Science or Cyber Forensic Unit/ Central Forensic Lab | | |
| | | | |
| MeitY | MoC | NGO | Industry |
| CERT In | TRAI | CSAHO | NASSCOM |
| Sectoral CERTs | CDOT | Skills DA | DSCI |
| STQC | CAoI | ISAC | Cybersecurity Services and Products Firms including CG PSU/ Ordnance Factories |
| CDAC | MTNL | Cyber Peace Foundation | |
| CCA | BSNL | CACMP | |
| NIC | Other leading TSP/ ISP | CySI | |
| | | CECSRDI | |
| | | Cyber Swachhta Kendra | |
| | | NCS of India | |
| | | | |
| MHRD | MoF | Academia | Min of Shipping/ Tpt |
| NSDC | Few Banks | Specific Universities | LRT |
| UPSC | 02 x Stock Exchanges | Specific Think Tanks | Aviation |
| Employment Exchange | Few Financial firms | SETS, Chennai | Metro Rail |
| | GSTIN | | |
| | | | |
| State Govt | Students Attending Courses | DOS | |
| CISO, ISM | e.g. at ISAC, India | ISRO | |

*Table 6: Representative List of Potential Respondents from Organisations/ Establishments - which are principally engaged in Cybersecurity activities and hence may be deemed as key stake-holders in selection of Cybersecurity Talent (Source: (Chhibbar, 2020; DSCI & PwC, 2019; Saraswat, 2019))*

5.4. **Data Collection**. Data collection will be attempted through structured surveys based on a questionnaire (Likert Scale).

*5.5.* **Data Analyses**. Data analyses will be attempted using descriptive and inferential statistics; and parametric and non-parametric tests/ methods.

6. **Expected Outcome of the Research**.

Ideally, a **m**ulti-**d**imensional, **c**yber **t**alent-selection model, if put in place, can facilitate cyber talent selection across diverse cyber organisations. However, such a model, has not been postulated and validated, to the best of this research scholar's knowledge. Such a model can potentially be extended to cover the selection of prospective candidates ranging from freshers to mid-career lateral inductees, across a diverse range of organisations. Development and initial validation of a generalisable, modular, customisable multi-dimensional cyber talent selection model for the India's cyber workforce, is the expected outcome.

**References**.


ASD, A. S. D. (2020). *ASD Cyber Skills Framework v2.0*. https://www.cyber.gov.au/sites/default/files/2020-09/ASD-Cyber-Skills-Framework-v2.pdf

Barrick, R. M. (2005). Yes, Personality Matters: Moving on to More Important Matters. *Human Performance*, *18*(4), 1-13. https://doi.org/10.1207/s15327043hup1804

Batey, M., & Hughes, D. J. (2017). Individual Difference Correlates of Self-Perceptions of Creativity. In *The Creative Self* (pp. 185-218). https://doi.org/10.1016/b978-0-12-809790-8.00011-x

Bentler, P. M., & Chou, C.-P. (1987). Practical Issues in Structural Modeling. *Sociological Methods in Research*, *16*(No. 1), 40. https://doi.org/10.1177/0049124187016001004

Bollen, K. A. (1989). *Structural Equations with Latent Variables*. John Wiley & Sons.

Borman, W. C., & Motowildo, S. J. (1993). Expanding the Criterion Domain to Include Elements of Contextual Performance. In N. Schmitt & C. W. Borman (Eds.), (1993 ed., pp. 71-98). Jossey-Bass.

Campbell, S. G., & Bradley, P. (2018). What shape peg are you? Different cyber jobs require different cognitive skills. https://wsiw2018.l3s.uni-hannover.de/papers/wsiw2018-Campbell.pdf

Campbell, S. G., Saner, L. D., & Bunting, M. F. (2016a). *Characterizing cybersecurity jobs* Proceedings of the Symposium and Bootcamp on the Science of Security,

Campbell, S. G., Saner, L. D., & Bunting, M. F. (2016b). Characterizing cybersecurity jobs: Applying the Cyber Aptitude and Talent Assessment Framework. *Proceedings of the Symposium and Bootcamp on the Science of Security, HotSos '16*, 25-27.

Caulkins, B. D. (2018). Enhancements to Cybersecurity Curricula to Support Behavioral Aspects of Cyber. In (pp. 6-6).

Chambers, E., Foulon, M., Handfield-Jones, H., Hankin, S. M., & Hankin, S. M. (1998). The War for Talent. *McKinsey Quarterly 2017*(March), 44-57.

Chhibbar, D. A. (2020). *Navigating the Indian Cyberspace Maze: Guide for Policymakers*. KW Publishers Pvt Ltd and MP-IDSA. https://idsa.in/system/files/book/navigating-the-indian-cyberspace-book.pdf

Cook, M. (2016). *Personnel Selection* (Sixth ed., Vol. 4). Wiley Blackwell.

Cronbach, L. J. (1990). *Essentials of Psychological Testing* (5 ed.). Harper Collins.

DSCI, & PwC. (2019). *Cyber Security India Market: What Lies Beneath*. https://www.pwc.in/research-insights/2019/cyber-security-india-market.html

Fortson, C. C. L. (2017). Putting the Pieces Together: Army Cyber Warrior Talent Management. http://publications.armywarcollege.edu/pubs/3422.pdf

Galliano, J. (2017). Improved Matching of Cybersecurity Professionals' Skills to Job-Related Competencies: An Exploratory Study. https://doi.org/10.13140/RG.2.2.24121.88163

Holland, J. L. (1992). *Making vocational choices: A theory of vocational personalities and work environments* (2nd ed.). Psychological Assessment Resources.

Jacob, J., Ei, W., Sha, K., Davari, S., & Yang, A. (2018). Is the NICE Cybersecurity Framework (NCWF) Effective for a Workforce Comprised of Interdisciplinary Majors? *International Conference Scientific Computing*, 124-130.

Jose, I., LaPort, K., & Trippe, D. M. (2016). Requisite attributes for cyber security personnel and teams: Cyber risk mitigation through talent management. In S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J. A. Steinke (Eds.), (First ed., pp. 167-193). Routledge Falmer Press,Taylor & Francis Inc. https://doi.org/https://doi.org/10.4324/9781315796352

Kucharcikova, A. (2011). Human Capital - Definitions and Approaches. *International Scientific Journal of Human Resources Management and Ergonomics*, *V*(2), 11.

Lubinski, D. (2000). Scientific and social significance of assessing individual differences: "sinking shafts at a few critical points". *Annual review of psychology*, *51*, 405-444. https://doi.org/10.1146/annurev.psych.51.1.405

McClelland, D. C. (1973). Testing for competence rather than for "intelligence". *The American psychologist*, *28*(1), 1-14. https://doi.org/10.1037/h0034092

Meehl, P. E. (1990). Appraising and Amending Theories : The Strategy of Lakatosian Defense and Two Principles that Warrant It Appraising and Amending Theories : The Strategy of Lakato, 2009. *Psychological Inquiry: An International Journal for the Advancement of Psychological Theory*(February 2015), 37-41. https://doi.org/10.1207/s15327965pli0102

Minegishi, M. (2018). Talent management: Managing cybersecurity human resources. *NEC Technical Journal*, *12*(2), 94-98.

Morris, J., & Waage, E. (2015). Cyber aptitude assessment: Finding the next generation of enlisted cyber soldiers. *The Cyber Defense Review*, *16*, 6-11. http://www.cyberdefensereview.org/2015/11/16/cyber-aptitude/

Mueller-Hanson, R., & Garza, M. (2016). Selection and staffing of cyber security positions. In S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J. A. Steinke (Eds.), (First ed., pp. 194-216). Routledge Falmer Press,Taylor & Francis Inc. https://doi.org/https://doi.org/10.4324/9781315796352

Newhouse, W., Keith, S., Scibner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Nunnally, J. C., & Bernstein, I. (1994). *Psychometric Theory* (Third ed.). McGraw-Hill, Inc.

Patrick M. Wright, G. C. M. (2011). Exploring human capital: putting human back into strategic human resource management. *Human Resource Management Journal*, *21*(2), 12. https://doi.org/10.1111/j.1748-8583.2010.00165.x

Pulakos, E. D., Arad, S., Donovan, M. A., & Plamondon, K. E. (2000). Adaptability in the workplace: development of a taxonomy of adaptive performance. *J Appl Psychol*, *85*(4), 612-624. https://doi.org/10.1037/0021-9010.85.4.612

Sackett, P. R., & DeVore, C. J. (2001). Counterproductive behaviours at work. In N. Anderson, D. S. Ones, H. K. Sinangil, & V. Viswesvaran (Eds.), (pp. 145-164). Sage Publications.

Saner, L. D., Campbell, S., Bradley, P., Michael, E., Pandza, N., & Bunting, M. (2016, 2016). Assessing aptitude and talent for cyber operations.*Advances in Intelligent Systems and Computing* Cham.

Saraswat, D. V. K. (2019, July 2019). *Cyber Security* [Presentation]. Vigyan Bhawan, Cyber Security Conclave, NITI Ayog. https://niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf

Schmidt, E., & Rosenberg, J. (2014). *How google manages talent* https://hbr.org/2014/09/how-google-manages-talent

Schmidt, F. L., & Hunter, J. E. (1998). The Validity and Utility of Selection Methods in Personnel Psychology: Practical and Theoretical Implications of 85 Years of Research Findings. *Psychological Bulletin*, *124*(2), 262-274. https://doi.org/10.1037/0033-2909.124.2.262

Shuftan, M., & Michaud, J. (2016). Keeping your SOCs full: Strengthening capacity in cyber talent. The SysAdmin, Audit, Network and Security Institute. In. Bethesda, MD: SANS.

Singer, P. W., & Friedman, A. (2015). Cybersecurity and cyberwar: what everyone needs to know. *Choice Reviews Online*, *52*(09), 52-4806-4852-4806. https://doi.org/10.5860/choice.188472

Sjöberg, S. (2014). *Utilizing Research in the Practice of Personnel Selection* (Vol. Unpublished).

Snow, R. E. (1978). Theory and method for research on aptitude processes. *Intelligence*, *2*(3), 225-278. https://doi.org/10.1016/0160-2896(78)90019-3

Snow, R. E. (1992). Aptitude Theory: Yesterday, Today, and Tomorrow. *Educational Psychologist*, *27*(1), 5-32. https://doi.org/10.1207/s15326985ep2701_3

Su, R. (2020). The three faces of interests: An integrative review of interest research in vocational, organizational, and educational psychology. *Journal of Vocational Behavior*, *116*. https://doi.org/10.1016/j.jvb.2018.10.016

Viswesvaran, C., Schmidt, F. L., & Ones, D. S. (2005). Is there a general factor in ratings of job performance? a meta-analytic framework for disentangling substantive and error influences. *Journal of Applied Psychology*, *90*(1), 108-131. https://doi.org/10.1037/0021-9010.90.1.108

MANAV RACHNA
vidyapatrikshal

**Dr. O.P. Bhalla Central Library**
**Manav Rachna International Institute of Research and Studies**
*(A deemed-to-be-university under section 3 of UGC Act 1956)*

---

## SIMILARITY VERIFICATION CERTIFICATE

---

Title: Staffing India's Cyber Workforce : Developing a multi-dimensional Cyber Talent - Selection Model

Researcher: Ramesh Balan

Registration Number: 19/PhD/065

Supervisor: Dr Nandini Srivastava

Department: FMS

This is to certify that the above mentioned Short Synopsis/Thesis was scanned for similarity index through Turnitin Software on 08 Mar 22 with submission ID 1779477545 and the similarity index was found to be 5 %. The complete report running into 30 Pages, 6122 Word count with File Size 3879 KB is being forwarded to the Research Supervisor/DRC/DRB for review.

MRIIRS Faridabad ★ Dr O P BHALLA CENTRAL LIBRARY ★
8/3/22

Excluding matches less than 14 words
Excluding matches less than 14 words

Date: 08 Mar 2022

---

The complete report of the above Short Synopsis/Thesis has been reviewed and the similarity index is below the accepted norms as per the University Grants Commission (Promotion of Academic Integrity and Prevention of Plagiarism in Higher Educational Institutions) Regulations 2018. The Short Synopsis/Thesis may be considered for further processing

08 Mar 22

Research Scholar

8/3/22

Research Supervisor